UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RAYCINE SOMMERS, individually and on behalf of all others similarly situated, Plaintiff, v. SOMNIA, INC. and ANESTHESIA SERVICES OF SAN JOAQUIN PC Defendants.	Case No.: 7:22-cv-10572 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Raycine Sommers ("Plaintiff"), individually and on behalf of a class of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to Plaintiff and on information and belief as to all other matters, and upon the investigation conducted by Plaintiff's counsel, alleges as follows:

PRELIMINARY STATEMENT

1. On or about July 11, 2022, Defendant Somnia, Inc. ("Somnia") belatedly detected hackers within its systems. These unauthorized attackers compromised Somnia's systems and made off with Plaintiff and Class Members' name, date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnostic information.

2. Somnia is an anesthesiology services provider and practice management company that manages numerous anesthesiology providers, including Defendant Anesthesia Services of San Joaquin PC ("Anesthesia Services"). In this role, Somnia obtains and holds numerous individuals'

personally identifiable information ("PII") and private health information ("PHI") from its anesthesiology providers.

3. While Somnia has been far from forthcoming about the details of its July 11, 2022 discovery (the "Data Breach"), its system was compromised by attackers to the point that it required "a global password reset, tightening firewall restrictions, and implementing endpoint threat detection and response monitoring software on workstations and servers." These myriad remediation measures demonstrate the breadth of Somnia's system's deficiencies. And, unsurprisingly given the overwhelming security failures, Anesthesia Services informed Plaintiff that "[Somnia's] investigation found that some information stored on the management company's systems may have been compromised."

4. On or about October 24, 2022, fifteen different anesthesiology practices spread across the country announced that their patients' information was part of the Data Breach involving their unnamed "management company," subsequently revealed to be Somnia. On November 7, 2022, additional anesthesiology practices, including Anesthesia Services, announced that their patients were also victims of the Data Breach.

5. As of the filing of this complaint, more than 450,000 individuals' information was affected in the Data Breach.

Breached Entity	**Individuals Affected**
Providence WA Anesthesia Services	98,643
Palm Springs Anesthesia Services	58,513
Anesthesia Services of San Joaquin	44,015
Anesthesia Associates of El Paso	43,168
Resource Anesthesiology Associates PC	37,687

Resource Anesthesiology Associates of IL	18,321
Bronx Anesthesia Services	17,802
Resource Anesthesiology Associates of CA	16,001
Grayling Anesthesia Associates	15,378
Hazleton Anesthesia Services	13,607
Anesthesia Associates of Maryland	12,403
Somnia Pain Mgt of Kentucky	10,849
Primary Anesthesia Services	9,517
Upstate Anesthesia Services	9,065
Resource Anesthesiology Associates of KY	8,980
Saddlebrook Anesthesia Services	8,861
Fredericksburg Anesthesia Services	7,069
Lynbrook Anesthesia Services	3,800
Resource Anesthesiology Associates of VA	3,305
Resource Anesthesiology Associates of CT PC	3,123
Somnia, Inc.	1,326
Resource Anesthesiology Associates of CA PC	1,308
Mid-Westchester Anesthesia Services	707
Total	**450,512**[1]

[1] *Data Breach Impacts Two Dozen Anesthesia Providers*, Oct. 13, 2022, available at https://www.hipaajournal.com/data-breach-impacts-more-than-one-dozen-anesthesia-providers/ (accessed Dec. 12, 2022).

6. Anesthesia Services, and the other anesthesiology providers listed above, negligently entrusted their customers' PII and PHI with Somnia.

7. Defendants have a duty to safeguard and protect customer information entrusted to them and could have prevented this theft with adequate security measures in the case of Somnia and by limiting the customer information it shared with its vendors and business associates in the case of Anesthesia Services.

8. Plaintiff and Class Members entrusted Defendants with, and allowed Defendants to gather, highly sensitive information relating to their health and other matters as part of seeking treatment. They did so in confidence, and they had the legitimate expectation that Defendants would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who were equipped to protect it.

9. Trust and confidence are key components of Plaintiff's and Class Members' relationship with Defendants. Without it, Plaintiff and Class Members would not have provided Defendants with, or allowed Defendants to collect, their most sensitive information in the first place; i.e., Plaintiff and Class Members relied upon Defendants to keep their information secure (as Defendants are required by law to do).

10. Plaintiff brings this class action because Defendants collected and failed to secure and safeguard numerous anesthesiology patients' PHI and PII—such as Plaintiff's and Class Members' names, date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnostic information (all collectively referred to as "Personal Information").

11. More than 450,000 anesthesiology patients have had their Personal Information compromised because of the Data Breach. As a result of Defendants' failure to protect the consumer information they were entrusted to safeguard, Plaintiff and Class Members suffered a loss of the value of their Personal Information—and have been exposed to or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

12. Defendants' intentional, willful, reckless, unfair, and negligent conduct—failing to prevent the breach, failing to limit its severity, and failing to detect it in a timely fashion—harmed Plaintiff and Class Members uniformly. For this reason, Defendants should pay for monetary damages, for appropriate identity theft protection services, and reimburse Plaintiff for the costs caused by Defendants' substandard security practices and failure to timely disclose the same. Plaintiff is likewise entitled to injunctive and other equitable relief that safeguards her information, requires Defendants to significantly improve their data security, and provides independent, expert oversight of Defendants' security systems.

13. Defendants have also been unfairly and unjustly enriched because of their improper conduct, such that it would be inequitable for them to retain the benefits conferred upon them by Plaintiff and the Class Members. Plaintiff never would have engaged her anesthesiology providers to perform medical services and entrusted Defendants with her Personal Information, had she known that Defendants would permit unauthorized access to her Personal Information by Defendants' complete and utter disregard for security safeguards and protocols. Plaintiff would have used another provider.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendants are citizens of States different from that of at least one Class Member.

15. This Court has personal jurisdiction over Somnia because it maintains its principal place of business in this District. Somnia is authorized to and regularly conducts business in New York. Somnia makes decisions regarding corporate governance and management of its blood testing labs in this District, including decisions regarding the security measures to protect its customers' Personal Information.

16. This Court has personal jurisdiction over Anesthesia Services because it regularly conducts business in New York and has sufficient minimum contacts in New York such that Anesthesia Services intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because each of the Defendants transact business and may be found in this District. Specifically, Somnia's principal place of business is located in this District and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Defendants' governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Data Breach. Further, Anesthesia Services lists a New York mailing address in Harrison, New York on its National Provider Identifier information.

PARTIES

18. Plaintiff Raycine Sommers is a natural person residing in Stockton, California. Plaintiff Sommers is a Data Breach victim who received a copy of the Breach Notice from Anesthesia Services on October 24, 2022.

19. Defendant Somnia, Inc. is a New York corporation with its principal place of business in Harrison, New York.

20. Defendant Anesthesia Services of San Joaquin, P.C. is a California corporation with its business address in Harrison, New York.

FACTUAL ALLEGATIONS

A. Defendants' Collection of PII and PHI

21. Somnia is an anesthesiology services provider and practice management company that owns and manages numerous anesthesiology practices across the United States. It states on its website that its vision is "to be the smartest choice in anesthesia practice management for healthcare facilities across the country."[2]

22. Anesthesia Services, per its National Provider Identifier information supplied to the State of California, is a "single specialty business group with one or more individual providers who practice in the same area of specialization."[3] Its NPI profile lists Dr. Marc E. Koch as its "President and CEO."[4] Dr. Marc E. Koch is also the CEO and President of Somnia.[5] Additionally,

[2] Somnia, Our Mission, https://somniaanesthesiaservices.com/somnia-anesthesia/company-mission/ (last accessed Dec. 12, 2022).
[3] NPI Profile, Anesthesia Services of San Joaquin, P.C., https://npiprofile.com/npi/1366778227 (last accessed Dec. 12, 2022).
[4] *Id.*
[5] Somnia, Executive Team, Marc E. Koch, https://somniaanesthesiaservices.com/executive-team/marc-e-koch-md-mba/ (last accessed Dec. 12, 2022).

Anesthesia Services' registered mailing address in Harrison, New York is the same address as Somnia's corporate headquarters.

23. The anesthesiology practices that Somnia works with obtains Class Members' PII and PHI when patients receive anesthesiology. This includes, upon information and belief:

a. Contact information;

b. Authentication information such as driver's licenses and Social Security Numbers;

c. Demographic information;

d. Payment information; and

e. Medical history as reported by patients and/or other healthcare providers.

24. Obtaining this information is a precondition of receiving anesthesiology services.

25. Anesthesia Services collects and maintains patient and former patient PII and PHI. This information subsequently gets transferred to Somnia.

B. The Data Breach

26. On July 11, 2022, Somnia belatedly discovered "suspicious activity on its systems."[6] While Somnia did not disclose what led it to this discovery or what the suspicious activity was, its notices nevertheless indicated that its attempted remediation required it to "disconnect[] all systems" and to undertake a "global password change," "tighten[] firewall restrictions, and deploy[] endpoint threat detection and response monitoring software on workstations and servers."[7]

[6] Somnia, Security Incident, https://somniaanesthesiaservices.com/somnia-anesthesia/security-incident/ (last accessed Dec. 12, 2022).
[7] *Id.*

27. The need to tighten firewall restrictions indicates that the hackers were able to install malware that provided them with a "backdoor" into Somnia's system wherein they could roam freely without detection throughout Somnia's systems. This demonstrates that there was a total breach of Somnia's systems.

28. Further, the need to deploy endpoint threat detection demonstrates that either Somnia: (1) did not have antivirus software installed on its servers and workstations (in violation of every basic security requirement) or (2) its patchwork antivirus software failed to detect the hackers. Either way, having effective antivirus software is a basic security precaution that any company must employ, particularly one such as Somnia that holds patients' PHI.

29. The result of Somnia's investigation was stark. The investigation revealed that information may have been compromised and the information taken included all of the PII and PHI detailed above.

30. On September 22, 2022, Somnia informed Anesthesia Services of the breach and stated on its website that it provided notice to "impacted individuals on September 22 and 23, 2022, through substitute notice."[8]

31. On October 24, 2022, additional notice was sent to Plaintiff and Class Members from their specific anesthesiology providers, including Anesthesia Services. This notice provided the scant details above and offered identity theft protection services to recipients.

32. The information provided to the U.S. Department of Health and Human Services Office for Civil Rights Data Breach Portal listed the "location of breached information" as "network server," but otherwise did not contain additional information about the cause of the

[8] *Id.*

breach.[9]

C. Defendants' Deficient Notice

33. Somnia and Anesthesia Services' notices concerning the Data Breach were deficient both in their content and their unexplained tardiness.

34. Defendants' notices, which were substantively identical, do not provide critical information to Plaintiff and Class Members. They do not state how long the unauthorized attackers were inside of Somnia's systems, how unauthorized attackers were able to get inside Somnia's systems without detection, and how unauthorized attackers were able to exfiltrate Personal Information without detection.

35. Defendants' notices do not explain precisely what Personal Information was taken from each individual, stating broadly that "information stored in the Management Company's system could include some combination of patient names, addresses, health insurance policy number, Social Security numbers, payment information, and health information such as treatment and diagnosis."[10]

36. Furthermore, Defendants' notices failed to explain the extent to which the unauthorized attackers were able to compromise Somnia's systems. The notice vaguely states that Anesthesia Services was informed by Somnia of "suspicious activity."[11] In what way the activity was "suspicious" or how the activity was "identified" are unexplained.

37. The notice is also silent as to whether Plaintiff and Class Members' information is still being stored with Somnia. In fact, the notice from Anesthesia Services did not even name

[9] U.S. Dep't of Health & Human Servs. Office for Civil Rights, Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Dec. 12, 2022).
[10] *See* Ex. A, Oct. 24, 2022 Ltr. from Anesthesia Services to Plaintiff.
[11] *Id.* at 1.

Somnia, referring to it instead as a "management company."[12]

38. Numerous state laws required Defendants to provide prompt notice of the Data Breach. Defendants failed to do so. Somnia stated that the Data Breach was discovered on July 11, 2022. However, it was not until September 21 and 22, 2022 that Somnia even informed its contractual partner, Anesthesia Services.

39. Somnia did not provide any notice until September 22 and 23, 2022, in what it describes on its website as "substitute notice."[13] What actions it actually took are unclear.

40. It was not until October 24, 2022, that Anesthesia Services mailed letters to "impacted individuals." At that point, three months had passed and Plaintiff and Class Members were left wondering what of their information was taken. And this delay left Plaintiff and Class Members at least three months behind the unauthorized attackers who exfiltrated their Personal Information. Somnia informed the U.S. Department of Health and Human Services Office for Civil Rights Data Breach Portal that same date and placed the same vague language on its website.[14]

41. Plaintiff and Class Members are left trying to understand what happened with their Personal Information, what risks they face, and the time period during which their Personal Information was improperly taken.

D. Defendants Failed to Safeguard Patient PII and PHI

42. Defendants failed to exercise reasonable care in protecting patients' information.

43. Defendants have a non-delegable duty under federal law to ensure that all information they collect and store is secure, and that any associated entities with whom they shared

[12] *Id.*
[13] Somnia, Security Incident, https://somniaanesthesiaservices.com/somnia-anesthesia/security-incident/ (last accessed Dec. 12, 2022).
[14] *Id.*

information maintain adequate and commercially reasonable data security practices to ensure the protection of patients' Personal Information.

44. Indeed, Defendants' entire business depends on patients entrusting them with their Personal Information. Without patients' Personal Information, Defendants would not be able to perform any services and certainly would not be able to bill patients and their insurance companies and collect payment for services rendered. More specifically, to provide services to patients, Anesthesia Services knows that its patients must trust that it is keeping their health information private and secure. If Anesthesia Services' patients lack trust in it or knew it would insecurely store, safeguard, or transmit their personal information, then they will not disclose health information to it and will choose a different provider for services.

45. More specifically, to provide services to patients, Defendants must trust that the patients' health information is private and secure. If Anesthesia Services' patients lack trust in it or knew it would insecurely store, safeguard, or transmit their personal information or fail establish or follow data security policies and protocols, they will not disclose health information to it and will choose a different provider for services.

46. This is why Defendants are entities covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), *see* 45 C.F.R. § 160.102, and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

47. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information"

which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

48. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

49. HIPAA requires that Defendants implement appropriate safeguards for this information.

50. HIPAA mandates that covered entities such as Defendants may disclose PHI to a "business associate," only if the covered entity obtains satisfactory assurances that the business associate, here Somnia, will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[15]

51. HIPAA further requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – i.e. non-encrypted data.

52. Somnia's vague notices indicate that it failed to detect unauthorized attackers, had information exfiltrated without detection, and that its security was so deficient that it required a "global password change, tightening firewall restrictions, and [the deployment of] endpoint threat detection and response monitoring software on workstations and servers."[16]

[15] *See* 45 CFR §§ 164.502(e), 164.504(e), 164.532(d) and (e).
[16] Somnia, Security Incident, https://somniaanesthesiaservices.com/somnia-anesthesia/security-incident/ (last accessed Dec. 12, 2022).

53. As detailed above, these remediation measures plausibly demonstrate that hackers were able to totally compromise Somnia's systems by installing malware that Somnia's antivirus software, to the extent it existed, failed to detect.

54. The unstated length of time between the Data Breach and Somnia's claimed discovery of the Data Breach indicates that Somnia's systems to detect intrusion, detect unusual activity, and log and report such events were inadequate and not in compliance with industry standards. For example, according to technology security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been trending downward in recent years—due to improvements in detection computer technology.[17] The fact that Somnia did not even disclose how long it took to detect the Data Breach is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiff's and Class Members' Personal Information.

55. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). It is unclear whether Defendants were encrypting payment card information according to minimum industry standards of PCI DSS.

56. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive

[17] *M-Trends 2019: FireEye Mandiant Services Special Report*, https://content.fireeye.com/m-trends/rpt-m-trends-2019 (last visited Dec. 12, 2022).

authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[18]

E. Defendants Violated HIPAA's Requirements to Safeguard Data and Regulatory Guidance

57. Defendants failed to maintain the privacy and security of their patients' PHI and failed to inform patients that their Personal Information was disclosed. Indeed, Defendants violated HIPAA by failing to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protect Plaintiff's and the Class Members' Personal Information;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in

[18] Securing Account Data with the PCI Point –to-Point Encryption Standard v2, https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last accessed Dec. 12, 2022).

violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

i. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

58. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[19]

59. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data. Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of

[19] FTC, *Start With Security: A Guide for Businesses*, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Dec. 12, 2022).

personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[20]

60. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[21]

61. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[22]

62. Defendants were fully aware of their obligations to implement and use reasonable measures to protect the PII and PHI of Anesthesia Services' patients, but failed to comply with these basic recommendations and guidelines that would have prevented the Data Breach from occurring.

---

[20] *Id*.
[21] *Id*.
[22] FTC, *Privacy and Security Enforcement*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last accessed Dec. 12, 2022).

F. Plaintiff and Class Members' Personal Information Is Highly Valuable

63. Defendants were or should have been aware that they were collecting highly valuable data, for which Defendants knew or should have known there is an upward trend in data breaches in recent years.[23]

64. The U.S. Department of Health and Human Services, Office for Civil Rights, lists the Data Breach as one of the largest healthcare breaches reported in 2022.[24]

65. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of threat actors, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[25]

66. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that "just the types of test proscribed might indicate a type of illness that you would not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet . . . having other information makes the data more valuable and the price higher."[26] Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches,

---

[23] Healthcare Data Breach Statistics, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last accessed Dec. 12, 2022) ("Our healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 10 years.").
[24] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Dec. 12, 2022).
[25] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS, Aug. 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last accessed Dec. 12, 2022).
[26] *Id.*

identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security numbers and other Personal Information directly on various dark web[27] sites making the information publicly available.[28]

67. Healthcare data is especially valuable on the black market. According to one report, a healthcare data record may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[29]

68. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[30]

69. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it,

[27] The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed Dec. 12, 2022).

[28] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Dec. 12, 2022); McFarland et al., *The Hidden Data Economy*, at 3, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last accessed Dec. 12, 2022).

[29] *Hackers, Breaches, and the Value of Healthcare Data* (June 20, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers/ (last accessed Dec. 12, 2022).

[30] Jim Finkle, *Your medical record is worth more to hackers your credit card*, Reuters, https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last accessed Dec. 12, 2022).

by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual."[31] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[32]

70. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[33]

G. Defendants Harmed Plaintiff And Class Members By Allowing Anyone To Access Their Information

71. Defendants knew or should have known both that medical information is incredibly valuable to threat actors and that health care data breaches are on the rise. Accordingly, Defendants were on notice for the harms that could ensue if they failed to protect patients' data.

---

[31] Andrew Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last accessed Dec. 12, 2022).

[32] Paul Nadrag, *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 12, 2022).

[33] *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web* (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited Dec. 12, 2022).

72. Given the sensitive nature of the Personal Information stolen in the Data Breach—including Social Security number, date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info—threat actors have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future.

73. In fact, it is likely that many victims of the Data Breach have already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. As detailed above, hackers were able to totally compromise Somnia's system, exfiltrate information, and companies like Somnia that hold patient PHI are frequent targets for hackers who then use the information to perpetrate identity theft on their victims. Plaintiff and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

74. The PII and PHI exposed in the Data Breach is highly coveted and valuable on underground or black markets—and information tied to this Data Breach has already been offered for sale. For example, identity thieves can use the stolen information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit

medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

75. While federal law generally limits an individual's liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[34] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[35]

76. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[36]

77. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with

[34] *Ponemon Institute, Fifth Annual Study on Medical Identity Theft*, https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 (last accessed Dec. 12, 2022).
[35] *Id*. at 9.
[36] *Id*. at 2.

19% responding that they missed out on employment opportunities as a result.[37]

78. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[38] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[39]

79. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits;
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[40]

80. Other types of medical fraud include "leveraging details specific to a disease or

[37] *Id*. at 14.
[38] *Id*. at 1.
[39] *Id*.
[40] *FTC, Medical Identity Theft FAQs for Health Care Providers and Health Plans*, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last accessed Dec. 12, 2022).

terminal illness, and long-term identity theft."[41] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[42] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

81. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[43]

82. In addition, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-16 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[44] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-

[41] Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last accessed Dec. 12, 2022).
[42] *Id*.
[43] *Id.*
[44] Identity Theft Resource Center, *The Aftermath 2017*, https://web.archive.org/web/20200512124018/https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last accessed Dec. 12, 2022).

interest loan.

83. As explained further by the FTC, medical identity theft can have other serious consequences:

> Medical ID thieves may use your identity to get treatment – even surgery – or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[45]

84. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. identity theft and fraud resulting from the theft of their Personal Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling

[45] *Medical ID Theft: Health Information for Older People*, Federal Trade Commission, https://web.archive.org/web/20201019075254/https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last accessed Dec. 12, 2022).

and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts; and

h. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

85. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[46]

86. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[47]

87. Plaintiff and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that

[46] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed Dec. 12, 2022).
[47] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007), http://www.gao.gov/new.items/d07737.pdf (last accessed Dec. 12, 2022).

has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[48]

88. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendants would have no reason to tout their data security efforts to their actual and potential customers.

89. Consequently, had consumers known the truth about Defendants' data security practices—that they did not adequately protect and store their Personal Information—they would not have entrusted their Personal Information to Defendants.

FACTS SPECIFIC TO PLAINTIFF

90. Plaintiff is a citizen and resident of California.

91. She received anesthesia as part of a surgery in a California hospital in July 2021.

92. Plaintiff has no known relationship with Defendants other than having surgery in July 2021 under anesthesia and receiving a breach notice from Anesthesia Services on October 24, 2022.

93. In order to receive healthcare services, Plaintiff had to provide her Personal Information to Anesthesia Services.

94. Plaintiff did so and, upon information and belief, Anesthesia Services passed her information along to Somnia. She trusted that Defendants would use reasonable measures to protect her information, including complying with state and federal law.

95. Plaintiff has suffered harm as a result of the Data Breach. Specifically, she has spent

[48] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Mar. 21, 2022).

time dealing verifying the legitimacy of the breach notice, exploring credit monitoring, and placing an Experian fraud alert on her account.

96. Plaintiff has also faced a litany of identity theft since she provided her information to Defendants.

97. In the summer of 2022, she got an alert that she had voted in an election in Florida, despite not doing so and being a California resident.

98. In August 2022, she received a spam call informing her that a freeze was being placed on her Bank of America account.

99. In October 2022, she received a fraudulent text that her MasterCard credit card that she uses through Chase Bank had been frozen.

100. Additionally, Plaintiff has received spam text messages, emails, and calls since she provided her information to Defendants.

101. Plaintiff suffered actual injury in the form of damages to and diminution of the value of her Persona Information—which she entrusted to Defendants and which was compromised in the Data Breach.

102. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse from her Personal Information being accessed and exfiltrated by hackers. This injury was exacerbated by Defendants' delay in revealing the Data Breach.

103. Plaintiff has a continuing interest in ensuring that her Personal Information, which remains with Defendants, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

I. NATIONWIDE CLASS

104. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All natural persons residing in the United States whose Personal Information was compromised in the Data Breach.

105. The Nationwide Class asserts claims against Defendants for negligence (Count 1), negligence *per se* (Count 2), breach of confidence (Count 3), invasion of privacy – intrusion upon seclusion (Count 4), and unjust enrichment (Count 5).

106. The California Subclass is defined as:

> All natural persons residing in California whose Personal Information was compromised in the Data Breach.

107. The California Subclass, together with the Nationwide Class, are collectively referred to herein as the "Classes" or the "Class."

108. Excluded from the Class are Defendants, any entity in which either Defendant has a controlling interest, and either Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

109. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

110. **Numerosity. Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Defendants have acknowledged that hundreds of thousands of their customers' Personal Information has been compromised. Those individuals' names and addresses are

available from Defendants' records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of Class Members in the California Subclass, making joinder of all California Subclass members impracticable.

111. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendants had a duty to protect Personal Information;

b. Whether Defendants failed to take reasonable and prudent security measures;

c. Whether Anesthesia Services knew or should have known of the susceptibility of Somnia's systems to a data breach;

d. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendants' security measures to protect their systems were reasonable in light known legal requirements;

f. Whether Defendants' efforts (or lack thereof) to ensure the security of patients' Personal Information were reasonable in light of known legal requirements;

g. Whether Defendants' conduct constituted unfair or deceptive trade practices;

h. Whether Defendants violated state law when they failed to implement reasonable security procedures and practices;

i. Which security procedures and notification procedures Defendants should be required to implement;

j. Whether Defendants violated California consumer protection and medical information privacy laws in connection with the actions described herein;

k. Whether Defendants failed to notify Plaintiff and Class Members as soon as practicable and without delay after the data breach was discovered;

l. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach and/or the loss of the Personal Information of Plaintiff and Class Members;

m. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their Personal Information; and

n. Whether Plaintiff and Class Members are entitled to damages or injunctive relief.

112. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class Members. Plaintiff's Personal Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class Members and Plaintiff seeks relief consistent with the relief of the Class.

113. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class

actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

114. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

115. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendants or would be dispositive of the interests of members of the proposed Class.

116. **Ascertainability.** The Class and Subclass is defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class.

The Class and Subclasses consist of individuals who received services and whose information was supplied to Somnia. Class membership can be determined using Somnia's records in its databases, which is presumably also how Somnia and its anesthesiology providers were able to provide notice of breach letters to Plaintiff and Class Members.

117. **Injunctive Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

118. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendants failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiff and the Class Members;

c. Whether Anesthesia Services failed to adequately monitor and audit the data security systems of Somnia;

d. Whether Defendants were unfairly and unjustly enriched as a result of their improper conduct, such that it would be inequitable for Defendants to retain the benefits conferred upon them by Plaintiff and the other Class Members; and

e. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiff and the Nationwide Class against Defendants

119. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

120. Defendants required Plaintiff and Class Members to submit Personal Information to anesthesiology services, which Anesthesia Services and Somnia's other anesthesiology practices provided to Somnia. Defendants collected and stored the Personal Information for commercial gain.

121. Defendants knew or should have known that Somnia's systems were vulnerable to unauthorized access and exfiltration by third parties.

122. Defendants had a non-delegable duty to maintain adequate and commercially reasonable data security practices to ensure the protection of patients' Personal Information.

123. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' Personal Information within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

124. Defendants owed a duty of care to Plaintiff and Class Members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

125. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and the Plaintiff and Class Members. The special relationship arose because Plaintiff and Class Members entrusted Defendants with their confidential data as part of the health treatment process. Only Defendants were in a position to ensure that they had sufficient safeguards to protect against the harm to Plaintiff and Class Members that would result from a data breach.

126. Defendants' duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, as well as their own promises regarding privacy and data security to patients. This duty exists because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiff and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendants did not protect Plaintiff's and Class Members' information from threat actors.

127. Defendants' duties also arose under HIPPA regulations, which, as described above, applied to Defendants and establish national standards for the protection of patient information, including protected health information, which required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

128. Defendants' duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce,"

including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

129. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of their systems, and the importance of adequate security.

130. Defendants breached their common law, statutory, and other duties – and thus were negligent – by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

131. Defendants breached their duties to Plaintiff and Class Members in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

d. Failing to adequately monitor, evaluate, and ensure the security of Somnia's network and systems;

e. Failing to recognize in a timely manner that Plaintiff's and other Class Members' Personal Information had been compromised; and

f. Failing to timely and adequately disclose that Plaintiff's and Class Members' Personal Information had been improperly acquired or accessed.

132. Plaintiff's and Class Members' Personal Information would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

133. Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Personal Information.

134. It was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

135. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information.

136. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class Members suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take

years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

COUNT 2

NEGLIGENCE PER SE
On Behalf of Plaintiff and the Nationwide Class against Defendants

137. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

138. Defendants are entities covered by HIPAA (45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

139. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Anesthesia Services to obtain satisfactory assurances that its business associates, such as Somnia, would appropriately safeguard the protected health information it receives or creates on behalf of the Defendants. 45 CFR § 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA. Somnia constitutes a "business associate" within the meaning of HIPAA.

140. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiff and Class Members "without unreasonable delay" so that Plaintiff and Class Members can take appropriate measures to mitigate damages, protect against

adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410.

141. Defendants violated HIPAA by failing to reasonably protect Plaintiff's and Class Members' Personal Information, as described herein.

142. Defendants' violations of HIPAA constitute negligence per se.

143. Plaintiff and Class Members are within the class of persons that HIPAA was intended to protect.

144. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

145. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

146. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

147. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Somnia, including, specifically, the immense damages that would result to Plaintiff and Class Members.

148. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

149. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

150. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

151. As a direct and proximate result of Defendants' negligence per se under HIPAA and the FTC Act, Plaintiff and Class Members have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT 3

BREACH OF CONFIDENCE
On Behalf of Plaintiff and the Nationwide Class against Defendants

152. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

153. Plaintiff and Class Members maintained a confidential relationship with Defendants whereby Defendants undertook a duty not to disclose the Personal Information provided by Plaintiff and Class Members to Defendants to unauthorized third parties. Such Personal Information was confidential and novel, highly personal and sensitive, and not generally known.

154. Defendants knew Plaintiff's and Class Members' Personal Information was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the Personal Information they collected, stored, and maintained.

155. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's

and Class Members' Personal Information in intentional, knowing, and or negligence breach of this duty. The unauthorized disclosure occurred because Defendants failed to implement and maintain reasonable safeguards to protect the Personal Information in their possession and failed to comply with industry-standard data security practices.

156. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

157. As a direct and proximate result of Defendants' breach of confidence, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT 4

INVASION OF PRIVACY – INTRUSION UPON SECLUSION
On Behalf of Plaintiff and the Nationwide Class against Defendants

158. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

159. Defendants intentionally intruded into Plaintiff's and Class Members' seclusion by storing their Personal Information in a system that was unequipped and unable to keep their Personal Information secure.

160. By failing to keep Plaintiff's and Class Members' Personal Information secure, and disclosing Personal Information to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, *inter alia*:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized

persons;

c. failing to adequately secure their Personal Information from disclosure to unauthorized persons; and

d. enabling the disclosure of their Personal Information without consent.

161. The Personal Information that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial, health, and treatment information.

162. As a direct and proximate result of Defendants' intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT 5

UNJUST ENRICHMENT
On Behalf of Plaintiff and the Nationwide Class against Defendants

163. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

164. For years and continuing to today, Defendants' business model depended upon patients entrusting them with their Personal Information. Trust and confidence are critical and central to both the services provided by Defendants to patients and the billing and collection for such services. Unbeknownst to Plaintiff and Class Members, however, Defendants failed to reasonably or adequately secure, safeguard, and otherwise protect Plaintiff's and Class Members' Personal Information. Defendants' deficiencies described herein were contrary to their security messaging.

165. Plaintiff and Class Members engaged Defendants for services and provided Defendants with, and allowed Defendants to collect, their Personal Information on the mistaken

belief that Defendants complied with their duty to safeguard and protect patients' Personal Information. Defendants knew that the manner in which they maintained and transmitted patients' Personal Information violated their fundamental duties to Plaintiff and Class Members by disregarding industry-standard security protocols to ensure confidential information was securely transmitted and stored.

166. Defendants had within their exclusive knowledge at all relevant times the fact that they had failed to implement adequate security measures to keep patients' Personal Information secure. This information was not available to Plaintiff, Class Members, or the public at large.

167. Defendants also knew that Plaintiff and Class Members expected that their information would be kept secure against known security risks vetted before they received patients' Personal Information. And based on this expectation and trust, Defendants knew that Plaintiff and Class Members would not have disclosed health information to them and would have chosen a different provider for services.

168. Plaintiff and Class Members did not expect that Defendants would store or transmit their Personal Information insecurely.

169. Had Plaintiff and Class Members known about Defendants' deficient security practices, Plaintiff and Class Members would not have engaged Defendants to perform any services and would never have provided Defendants with their Personal Information.

170. By withholding these material facts, Defendants put their own interests ahead of their patients' interests and benefitted themselves to the detriment of Plaintiff and Class Members.

171. As a result of their conduct as alleged herein, Defendants sold more services than they otherwise would have and were able to charge Plaintiff and Class Members when they otherwise could not have. Defendants were unjustly enriched by charging and collecting for those

services to the detriment of Plaintiff and Class Members.

172. To be sure, this is not a question of whether Defendants misused patients' Personal Information. It is more foundational. Defendants promised to protect and safeguard Plaintiff's and Class Members' Personal Information at all times (from the inception of their relationship of trust and confidence) and never would have performed any services of value enabling them to bill or collect payment but for Defendants' unfair and deceptive practices.

173. It would be inequitable, unfair, and unjust for Defendants to retain these wrongfully obtained benefits. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

174. Defendants' defective security and their unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their private Personal Information.

175. Each Plaintiff and member of the proposed Classes is entitled to restitution and non-restitutionary disgorgement in the amount by which Defendants were unjustly enriched, to be determined at trial.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 6

CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code §§ 56, *et seq*. against Defendants

176. Plaintiff, individually and on behalf of the California Subclass, repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

177. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information

contained therein." Cal. Civ. Code § 56.101. "Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." *Id.*

178. The CMIA further requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

179. Plaintiff and California Subclass members are "patient[s]," "whether or not still living, who received health care services from a provider of health care and to whom medical information pertains" pursuant to § 56.05(j) of the CMIA.

180. Defendants are each a "provider of healthcare" pursuant to § 56.05(m) of the CMIA "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information."

181. Defendants are subject to the requirements and mandates of the CMIA and are therefore required to do the following under the CMIA:

a. Ensure that medical information regarding patients is not disclosed or disseminated or released without patients' authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.245, 56.26, 56.35, 56.36, and 56.101;

b. Not disclose medical information regarding a patient without first obtaining an authorization under Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, and 56.35;

c. Create, maintain, preserve, and store medical records in a manner that preserves the confidentiality of the information contained therein under Cal. Civ. Code §§ 56.06

and 56.101(a);

d. Protect and preserve confidentiality of electronic medical information in their possession under Cal. Civ. Code §§ 56.06 and 56.101(b)(1)(A); and

e. Take appropriate preventive actions to protect confidential information or records from unauthorized release under Cal. Civ. Code § 56.36I(2)(E).

182. The Personal Information of Plaintiff and California Subclass members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

183. The medical information compromised included Plaintiff's and California Subclass members' full names, dates of birth, Social Security numbers, driver's license information and genders, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis information.

184. Due to Defendants' negligent creation, maintenance, preservation and/or storage of Plaintiff's and the California Subclass members' electronic medical information, Defendants allowed Plaintiff's and California Subclass members' individually identifiable medical information to be accessed and actually viewed by at least one unauthorized third party, constituting a release in violation of Cal. Civ. Code § 56.101(b)(1)(A).

185. Defendants disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(i), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). Plaintiff and California Subclass members did not authorize Defendants' disclosure and release of their Personal Information that occurred in the Data Breach.

186. Defendants' negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and the California Subclass members' medical information in a manner that

preserved the confidentiality of the information contained therein violated the CMIA, Cal. Civ. Code §§ 56.06 and 56.101(a). Anesthesia Services transmitted patients' confidential medical information to Somnia which was then accessed, viewed, and exfiltrated by an unauthorized third party or parties, and thus Defendants negligently released medical information concerning Plaintiff and California Subclass members. Accordingly, Defendants' systems and protocols did not protect and preserve the integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code § 56.101.

187. Defendants violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiff's and California Subclass members' Personal Information; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and California Subclass members' Personal Information; (3) failing to use reasonable authentication procedures to track Personal Information in case of a security breach; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiff's and California Subclass members' Personal Information was kept.

188. Defendants' failure to implement adequate data security measures to protect the Personal Information of Plaintiff and California Subclass members was a substantial factor in allowing unauthorized parties to access Somnia's computer systems and acquire the Personal Information of Plaintiff and California Subclass members.

189. As a direct and proximate result of Defendants' violation of the CMIA, Defendants allowed the Personal Information of Plaintiff and California Subclass members to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be

accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and/or profit from their Personal Information, thereby breaching the confidentiality of their Personal Information. Plaintiff and California Subclass members have accordingly sustained and will continue to sustain actual damages as set forth above.

190. Plaintiff and California Subclass members were injured and have suffered damages, as described above, from Defendants' unauthorized release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and are therefore entitled to nominal damages of one thousand dollars ($1,000) for each violation under Civil Code §56.36(b)(1) or the amount of actual damages, if any, for each violation under Civil Code §56.36(b)(2).

191. Plaintiff and California Subclass members also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23, California Civil Code § 56.35, and California Code of Civil Procedure § 1021.5.

COUNT 7

CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §§ 17200, *et seq.*
On Behalf of the California Subclass against Defendants

192. Plaintiff, individually and on behalf of the California Subclass, repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

193. Defendants are "persons" as defined by Cal. Bus. & Prof. Code § 17201.

194. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

195. Defendants' "unfair" and "fraudulent" acts and practices include omitting, suppressing, and concealing the material fact that it did not have and did not reasonably ensure that Somnia reasonably or adequately secured Plaintiff's and California Subclass members' Personal Information.

196. Defendants engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, HIPAA, and California common law.

197. Defendants engaged in acts of deception and false pretense in connection with their accepting, collecting, securing, and otherwise protecting patient Personal Information and engaged in the following deceptive and unconscionable trade practices, including:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

d. Failing to adequately monitor and audit the data security systems of its vendors and business associates like Somnia;

e. Failing to adequately monitor, evaluate, and ensure the security of Somnia's network and systems;

f. Failing to recognize in a timely manner that Plaintiff's and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiff's and Class Members' Personal Information had been improperly acquired or accessed.

198. Plaintiff's and Class Members' Personal Information would not have been compromised but for Defendants' wrongful and unfair breach of its duties.

199. Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Personal Information.

200. Plaintiff and California Subclass members conferred a benefit on Defendants—payment for medical services—in reliance on Defendants' omissions and deceptive, unfair, and unlawful practices. Had Defendants disclosed in any form, whether verbally, in writing, or via electronic disclosure that they did not adequately secure patients' Personal Information, Plaintiff and California Subclass members would not have sought or purchased services from Defendants.

201. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein.

202. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their Personal Information; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 8

CALIFORNIA CONSUMER LEGAL REMEDIES ACT,
Cal. Civ. Code §§ 1750, *et seq.*
On Behalf of the California Subclass against Defendants

203. Plaintiff, individually and on behalf of the California Subclass, repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

204. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

205. Defendants are "persons" as defined by Civil Code §§ 1761(c) and 1770, and have provided "services" as defined by Civil Code §§ 1761(b) and 1770.

206. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

207. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

208. Plaintiff and California Subclass members are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

209. Defendants' acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including, but not limited to omitting, suppressing, and concealing the material fact that

they did not reasonably or adequately secure Plaintiff's and California Subclass members' Personal Information.

210. Defendants' omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' Personal Information.

211. Plaintiff and California Subclass members conferred a benefit on Defendants—payment for medical services—in reliance on Defendants' omissions. Had Defendants disclosed in any form, whether verbally, in writing, or via electronic disclosure that they did not reasonably adequately secure patients' Personal Information, Plaintiff and California Subclass members would not have sought or purchased services from Defendants.

212. Had Defendants disclosed to Plaintiff and California Subclass members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced employ systems with reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and California Subclass members' Personal Information as part of the services they provided without advising Plaintiff and California Subclass members that their data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and California Subclass members' Personal Information. Accordingly, Plaintiff and California Subclass members acted reasonably in relying on Defendants' omissions, the truth of which they could not have discovered.

213. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

214. Plaintiff and California Subclass members provided notice of their claims for damages to Defendants on December 13, 2022, in compliance with California Civil Code § 1782(a). If Defendants do not cure within 30 days—and Plaintiff does not believe curing is possible on this set of facts and circumstances—Plaintiff intends to amend this Complaint to seek statutory damages under the CLRA. Cal. Civ. Code § 1782.

215. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT 9

CALIFORNIA CONSUMER PRIVACY ACT, Cal. Civ. Code § 1798.150

On Behalf of the California Subclass against Defendants

216. Plaintiff, individually and on behalf of the California Subclass, repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

217. In the alternative to her CMIA claim, if Defendants are not deemed "providers of health care governed by the Confidentiality of Medical Information Act [] or a covered entity governed or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability

and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5)," Cal. Civ. Code § 1798.145(c)(A)(B), Plaintiff brings claims against Defendants for violating the California Consumer Privacy Act, Cal. Civ. Code § 1798.150.

218. Defendants violated § 1798.150 of the CCPA because their failure to implement and maintain reasonable security procedures and practices to protect Plaintiff's and California Subclass members' Personal Information. Defendants' failure was the direct and proximate result of Plaintiff's and California Subclass members' Personal Information being subject to unauthorized access and exfiltration, theft, or disclosure.

219. Upon information and belief, Defendants are "businesses" as defined by the CCPA, Cal. Civ. Code § 1798.140(c), that collect Personal Information for a "business purpose." Cal. Civ. Code § 1798.140(d).

220. Plaintiff and California Subclass members are "consumers" as defined by the CCPA. Cal. Civ. Code § 1798.140(e).

221. Plaintiff and California Subclass members' "personal information," as that term is defined by the CCPA, was part of the unauthorized access and exfiltration, theft, and disclosure. Cal. Civ. Code § 1798.150(a)(1) (defining "personal information" per Cal. Civ. Code 1798.81.5(d)(1). Specifically, the personal information includes Plaintiff and California Subclass members' names in combination with their Social Security number, Driver's license number, Medicaid ID, Medicare ID, and financial information. Cal. Civ. Code 1798.81.5(d)(1)(A)(i)-(iii).

222. Pursuant to California Civil Code 1798.150(b), on December 13, 2022 Plaintiff mailed a CCPA notice letter to Defendants, identifying the specific provisions of the CCCPA that violated. If Defendants do not cure the noticed violation within 30 days—which Plaintiff does not

believe is possible given the alleged facts and circumstances—then Plaintiff will promptly amend her complaint to seek statutory damages under Cal. Civ. Code 1798.150(a)(1)(A).

REQUESTS FOR RELIEF

Plaintiff, individually and on behalf of members of the Class, as applicable, respectfully requests that the Court enter judgment in her favor and against Defendants, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiff and Class Members compensatory, consequential, and general damages in an amount to be determined by a jury at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

7. That the Court award pre- and post-judgment interest at the maximum legal rate; and

8. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

By:/s/ *Jason L. Lichtman*

Dated: December 14, 2022

Michael W. Sobol (pro hac vice forthcoming)
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Email: msobol@lchb.com

Jason L. Lichtman
Sean A. Petterson
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, New York 10013
Telephone: 212.355.9500
Email: jlichtman@lchb.com
spetterson@lchb.com